An ISP Perspective from Atos: Attackers Think About Value – Do You?

Too often security is focused on silos and products. Too seldom does it regard the big picture, which is almost invariably about preserving value or money. Inversely, attackers often seem to have their priorities "straight" with one target in mind; and it isn't the intrusion protection system (IPS) or a server, per se. It's money. Sometimes they pursue that goal through extortion and ransom ("pay us or we take down your web site"). Other times, they sell exfiltrated intellectual property or passwords on the Dark Web. In other instances, they launch a DDoS attack simply to distract security staff while they steal money through illicit digital transactions.

It adds up to an important question: Is tackling security in a piecemeal fashion—focusing on server integrity software, next-generation firewalls, advanced threat detection appliances and so on—the optimal way to erect an impenetrable "wall" of security?

Clearly, security products such as DDoS mitigation appliances must be acquired and implemented. However, it is becoming imperative to approach security by first considering the value that is at stake—and determining how that value could "leak" out of the company. With that understanding, an organization must assume that hackers are already in. The question therefore is not "How do we keep them out?" but rather "How do we know they are in, and what do we do once they are?"

The history of IT and IT security is full of an evolving series of products designed to keep a company secure. Far more recent is the understanding that detection is insufficient; preparation and remediation are at least as important. In other words, it's not just about avoiding injury, but also stopping the bleeding ASAP.

DDoS attacks offer a prime example. Given the ease with which DDoS attacks can be launched, the acquisition and operation of world-class DDoS products and services is not optional. But it must also be remembered that DDoS attacks themselves are not always the ultimate goal. The goal is often financial: to hold a company to ransom, or to distract security staff while pilfering funds.

The security market is now using terms like “breach detection systems” and “security analytics” to describe how businesses must think about security in 2016. The focus is no longer merely prevention; it’s combining information from multiple sources to determine if an attack is occurring, what is at stake, and how to both prioritize and remedy it. This is especially pertinent in today’s environment, with highly advanced malware available for sale, readymade and ready to go—along with attacks that can be extraordinarily complex, requiring months to fully launch and even longer to discover.

Coping with today’s style of attacker requires a different kind of approach. The starting point is business value—where are the greatest business risks? Many companies might not even know, for example, where their most important documents actually reside physically—on which server(s) and where those server(s) are physically located. Less likely is knowing who has access to those documents, and much less likely is knowing, with certainty, who has accessed those documents and when.

With a clear understanding of business needs, companies must implement some kind of correlation tool (“advanced analytics”). Correlation has become mandatory because of how modern malware functions—not necessarily intruding or making itself known, but operating just below the radar. Thus, each individual security product may not alert, but the overall picture (one type of behavior or activity in one environment, and a different type in another environment) might require further investigation when seemingly benign activities are correlated together.

One reason to invest in security products is not so much to prevent attacks by themselves, but to serve as feeds into the main “security brain,” the SIEM. This is not to say that individual tools are not needed or that they aren’t as useful as they used to be. In fact, all of these tools are as mandatory as ever—as DDoS attacks have never been more serious.

But in addition to those tools—and advanced analytics to pull them all together—a world-class defense also requires two other components. The first is a team of experts who actually know what attacks look like in 2016. These are professionals who work within a security operations center (SOC). They are able to diagnose suspicious activities and separate the noise from the genuine threats. Software can often help, but software by itself cannot reliably diagnose all situations. The second requirement: practiced, well-rehearsed attack and recovery scenarios. It is not enough to know that an attack is occurring (or has occurred); equally important is knowing next steps.

A multidisciplinary team can help deliver both of those components. Security and operational personnel will often have specialties (firewalls, day-to-day server management or identity management, for instance), and each individual alone may not be able to understand or remediate the threat. In fact, it would be rare for any individual to be able to identify and then remediate a threat on their own. Teamwork is essential since one person may know about networking while another understands applications. The network pro would not be the person to execute (or even know how to execute) changes to the application to remove the threat.

Companies require interdisciplinary teams with the experience and know-how to both design and interpret advanced analysis. This core team would be responsible for proactive and reactive risk management processes—seeing warning signs early and then remediating problems once they occur.

Learn More at DDoS Warriors

To know more about today’s attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware’s Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.